Attack on Configuration Data

Eric Lazarus/Stephen Green

Taxonomy:

Administrative, locale, legal

Applicability:

DRE, DRE with VVPT, any configurable electronic voting machine

Method:

The perpetrator must configure some machines to either discard ballots or count ballots when abandoned by the voter and to do so in violation of election law. These malevolently configured machines could be, for example, distributed to polling places likely to be unfriendly to the candidate or proposition the attackers are attempting to benefit.

Voters do abandon their ballots on occasion, either out of ignorance, carelessness, or confusion. DRE, DRE with VVPT machines permit this confusion because some voters, on seeing the review screen, could believe that it was reporting the vote they had cast and not the vote that they could cast if they press the red "vote" button (or in some other way indicate that the vote should be cast.)

The election officials, on finding a voting machine with an un-cast ballot, generally have a procedure to follow: Two poll workers working together are to go to the machine, insert the supervisor PEB, enter the "poll worker override" password and force the system to perform the programmed action for abandoned ballots.

Resource Requirements:

The attack is subtle enough that a single insider might well carry it off, with overall effectiveness determined by where the configuration files are maintained and controlled. That insider could be a county election official, voting system vendor, or contactor.

Outsiders could carry off this attack via a break-in to a warehouse or via many small break-ins to actual polling places, the latter being far less efficient.

Potential Gain:

? How many ballot abandonment cases are we likely to see?

Likelihood of Detection:

In the case of the cited FL elections, misconfiguration was not detected during the entire operational period from the original purchase and installation date. Typically, misconfiguration would not be detected until a forensic audit is conducted to validate election results.

Countermeasures:

Two-level configuration files or other ways to detect or prevent incorrect settings.

(see also countermeasure page on wiki to ensure we are covering relevant countermeasures already discussed)

Preventative Measures:

Centralized control of configuration files and a secure means of distributing the files out to the precincts. If local configuration is a requirement, a two person control process could be implemented where one person enters the required information and the second person verifies the information has been entered correctly. The configuration files are then hashed and recorded to address any post-election concerns.

Detection Measures:

Detection of configuration file errors could be accomplished through the use of setup validation, either automatically by file hash validation or manually through procedure. Printouts of the configuration files, pre- and post-election could be used to detect tampering or misconfiguration.

Attack Economics:

Small number of attackers. Number of votes that can be stolen this way is _____ (please fill in!) This would depend on where the configuration files are controlled and how many voters abandoned, by negligence or persuasion, their ballots.

(Please see BC attack catalog info for BC estimates of costs)

Variations on attack theme:

Attack on PCOS systems by turning off over vote protection. General concept is look to the handling of unusual cases because the human mind tends to focus on the normal case.

Other system configuration settings besides handling of abandoned ballots need to be evaluated, i.e. counter thresholds, randomization seed values, etc. The location where the configuration information is stored should also be evaluated, i.e. is it stored on removable media, in a flashable memory module, a protected directory on a local file system, etc.

This attack can be considered a form of Trojan Horse except that no computer skills or software modifications are need. A small percent of votes are never cast for the attacker's opposition due to a plausibly deniable incorrect configuration setting.
(e.g., what variations of this attack are there -- see BC attack catalogs for preliminary thoughts)

Conclusions:

Processes, procedures and technology that are not observable seem to create risks of fraud and of error both.

So, in this example, unlike the situation with conventional paper ballots, where an election observer could easily tell whether the pollworkers were placing that ballot in the ballot box, on the one hand, or in the trash can, on the other hand, nothing an observer could see would indicate what had happened to the ballot. In fact, it is not clear that a very knowledgeable pollworker could see what had happened.

Configuration settings which impact vote totals need to be overtly obvious to pollworkers, especially for abandoned ballots and the corresponding procedures and laws. During normal “poll worker override” operations, extra care and effort by the system designers is needed so that the display properly conveys the actions being taken with the ballots.

(i.e., countermeasures a, b and c likely to be most effective, countermeasure d inneffective because technology too expensive or not advanced enough)

Citations:

Miami-Dade Elections Supervisor Constance Kaplan resigned in March of 2005 because apparently, for at least one year Miami was using DRE systems the option had been set wrong, presumably not malevolently but due simply to the large number of settings and the fact that setting them right requires a detailed reading of the law and the ability to deal with nonobvious user interfaces in preparing the options file. There is lots of room for oversight and clerical error, and each county is on their own to get it.

While the legal responsibility sits squarely on the county election supervisor. The basic system design makes it at once very difficult for the commissioner to be sure that the law is being carried out and, at the same time very easy for another individual to expolite the volnerablity.

Miami-Dade elections chief quits under fire, Associated Press, April 2, 2005